# Exploring the use of Intel SGX for Secure Many-Party Applications

SysTEX'16

K. A. Kucuk

University of Oxford, UK

December 12, 2016

# Overview

1. Introduction
2. Trustworthy Remote Entity (TRE)
3. SGX-based TRE
4. Results

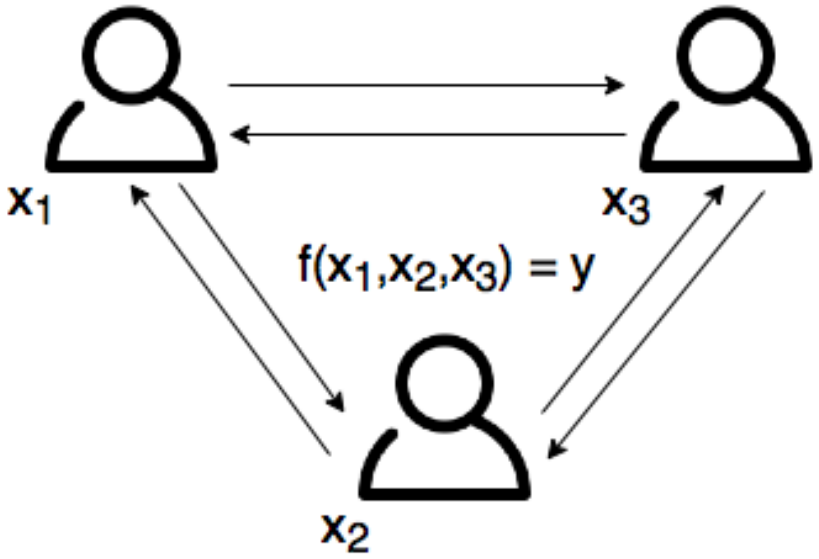
# Yao's Millionaires' Problem

x

y

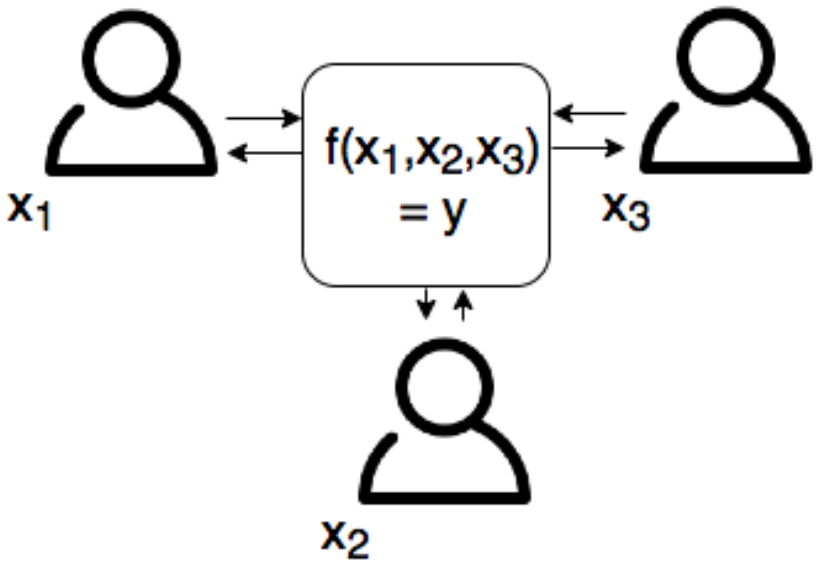
x > y ?

# Multi Party Computation (MPC)



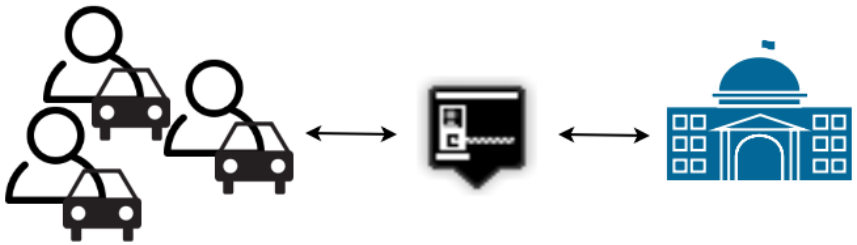

Limited scalability,
Cryptographic primitives

# Ideal MPC



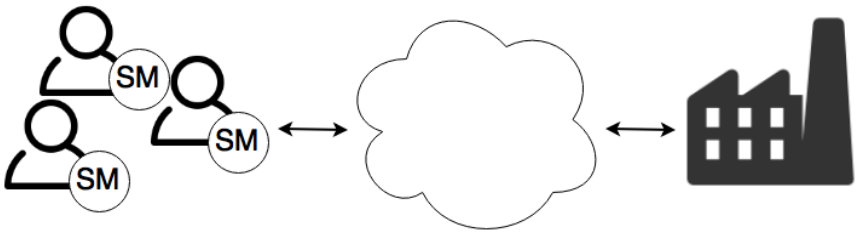

Third Party,
Trust Issues

# Many Party Application: Road Pricing



Location-based services
..diminishes the privacy

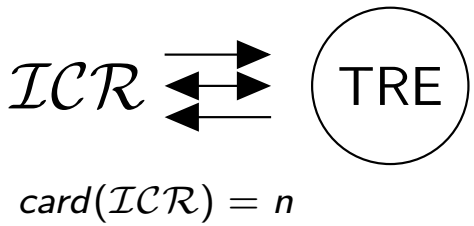
# Many Party Application: Smart Grid

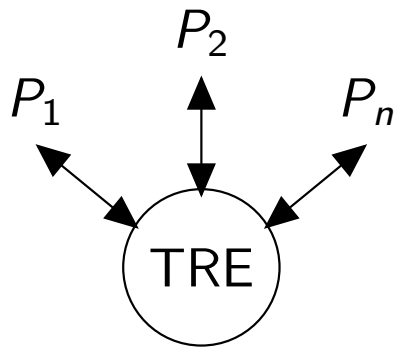



aggregate measurements
over multiple consumers

# A Possible Solution ...

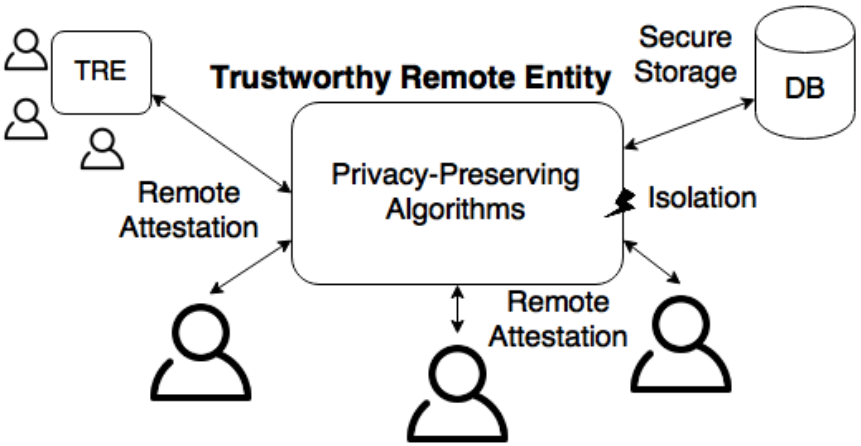
## Trustworthy Remote Entity (TRE)




- Based on Trusted Computing
- Essentially a verifiable trusted third party (vTTP)
- Comparable to the idealised version (TTP) in the MPC world

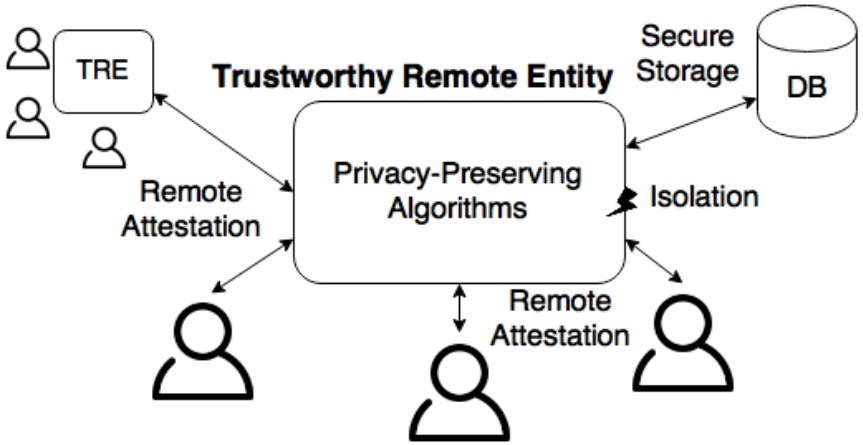
# TPM-based TRE




## Using TXT and TPM

- Final State Attestation (FSA)
- Bare-metal, event-driven
- Privacy Preserving
- Small TCB, Optimized

# Other TRE possibilities

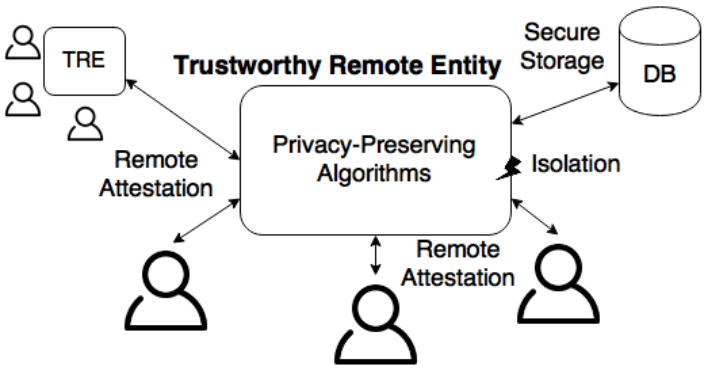



Intel SGX; sgxTRE,

Middlebox, Compute Provider

ARM TrustZone

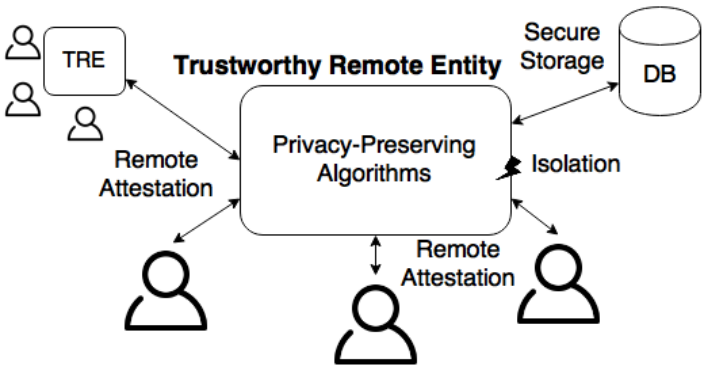
# Contributions




## SGX-based TRE

- SGX Benchmarks
- Design and Prototype
- Comparison

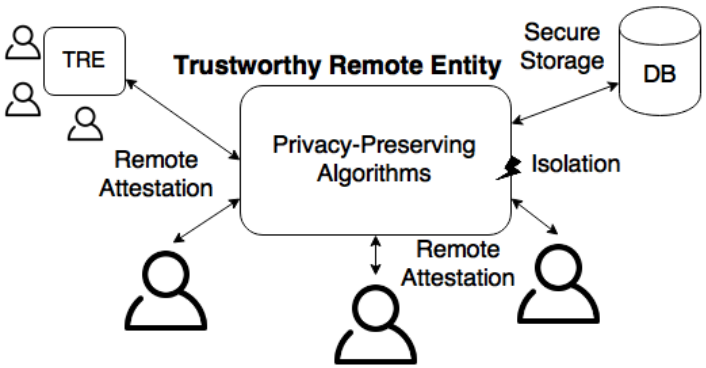
# Requirements




## Security and Performance Req.

- Secure Computation and Communication
- Secure Attestation
- Scalability and Latency

# Adversary Model



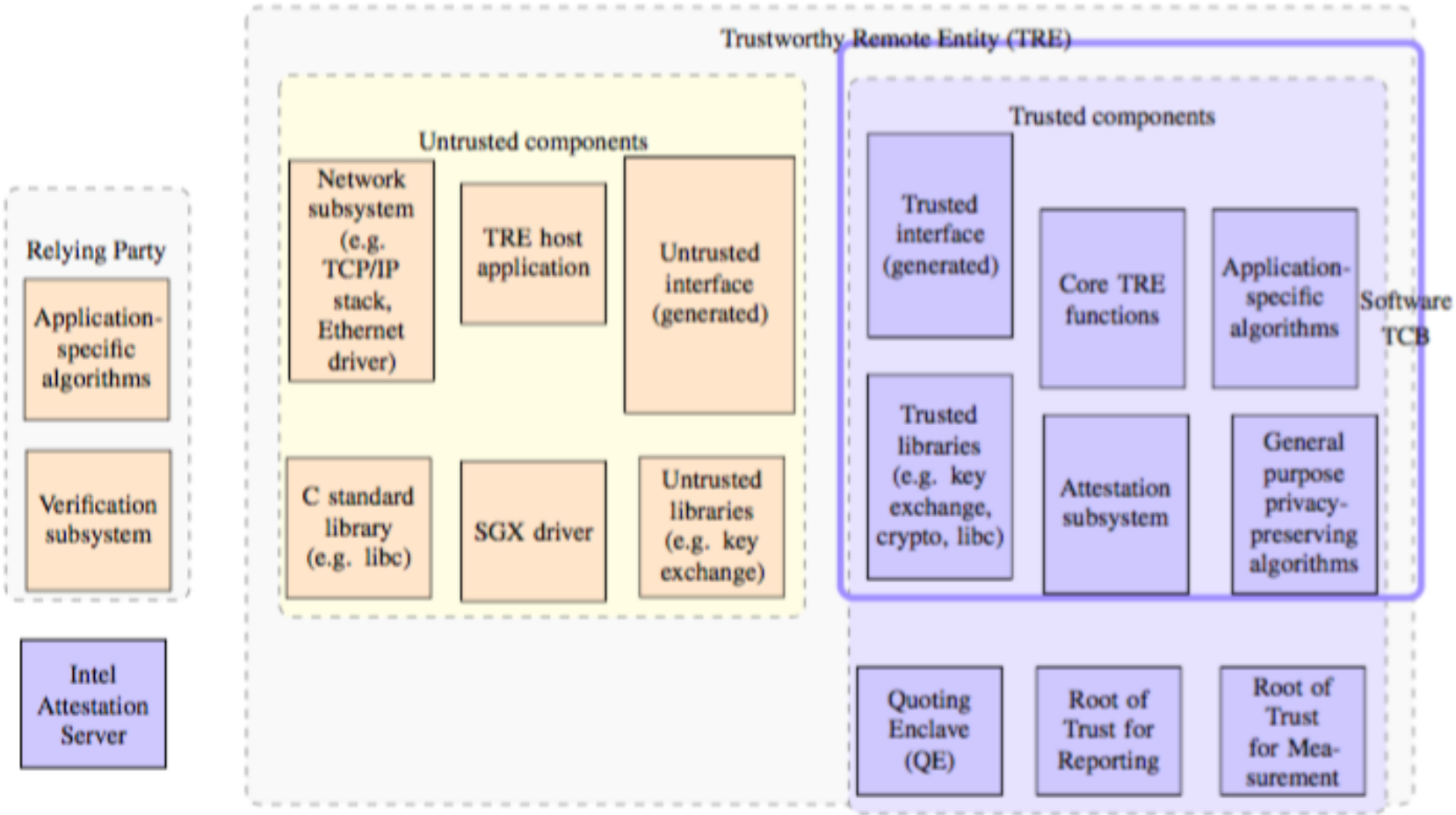

## Malicious Operator of TRE

- Dolev-Yao Network Adv.
- SMM, BIOS, OS
- Physical Access

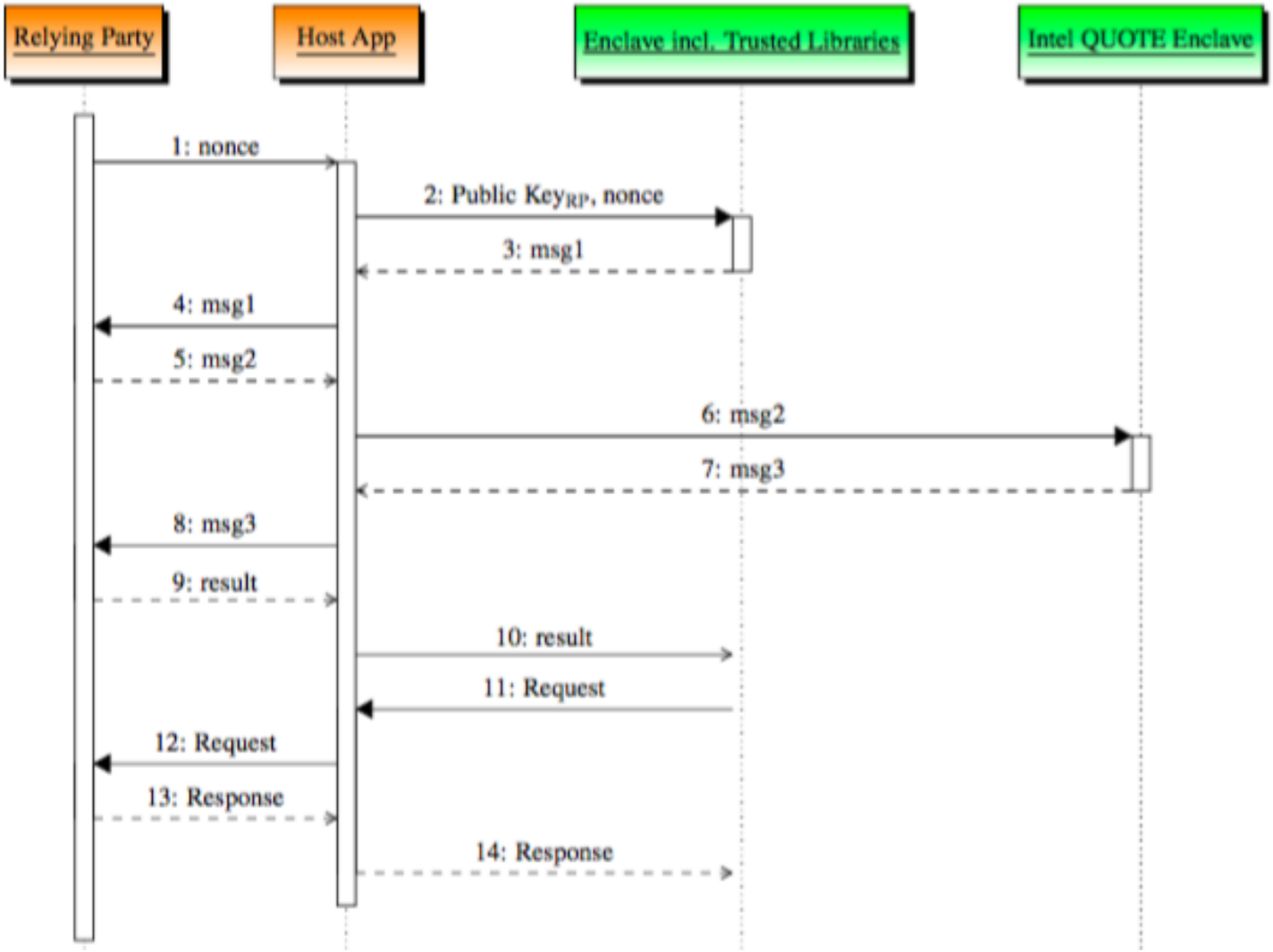
# Benchmarking Functionalities

| Operation | Stack+Heap | Mean (ms) | Std Dev (ms) |
|---|---|---|---|
| Create Enclave | 20 kB | 9.986 | 0.488 |
| | 5 MB | 24.558 | 2.154 |
| Initialize Remote Attestation | 20 kB | 0.040 | 0.004 |
| | 5 MB | 0.055 | 0.012 |
| Initialize Secure Channel | 20 kB | 0.511 | 0.056 |
| | 5 MB | 0.611 | 0.083 |
| Quote & SIGMA Protocol | 20 kB | 33.059 | 1.968 |
| | 5 MB | 31.764 | 1.250 |
| Destroy Enclave | 20 kB | 0.116 | 0.060 |
| | 5 MB | 1.158 | 0.103 |

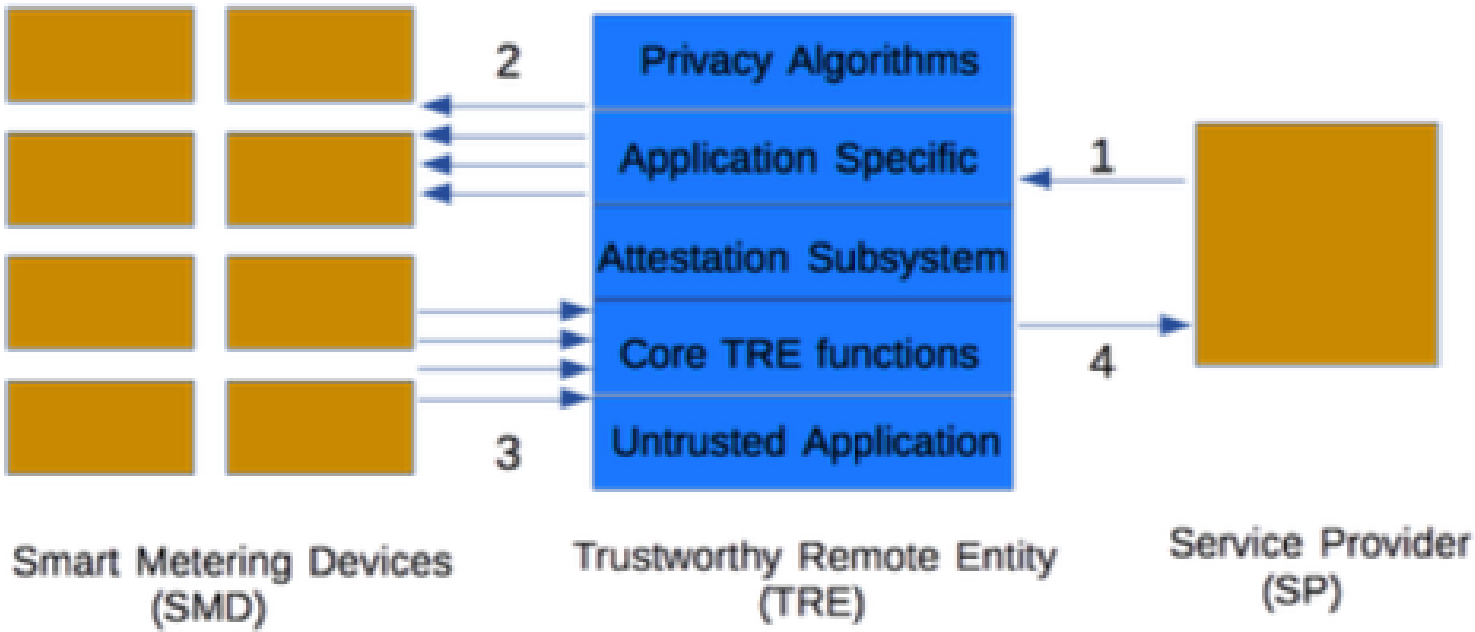
# Implementation: Architecture



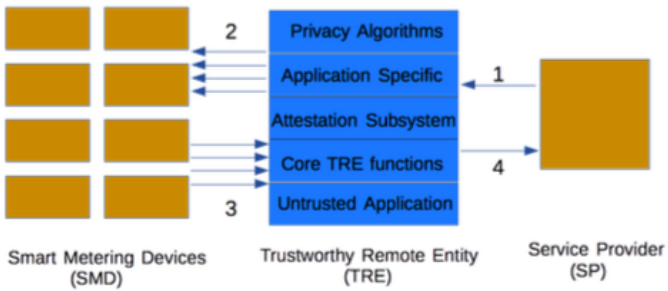
# Implementation: Flow



# Implementation: Abstract



# Experiment



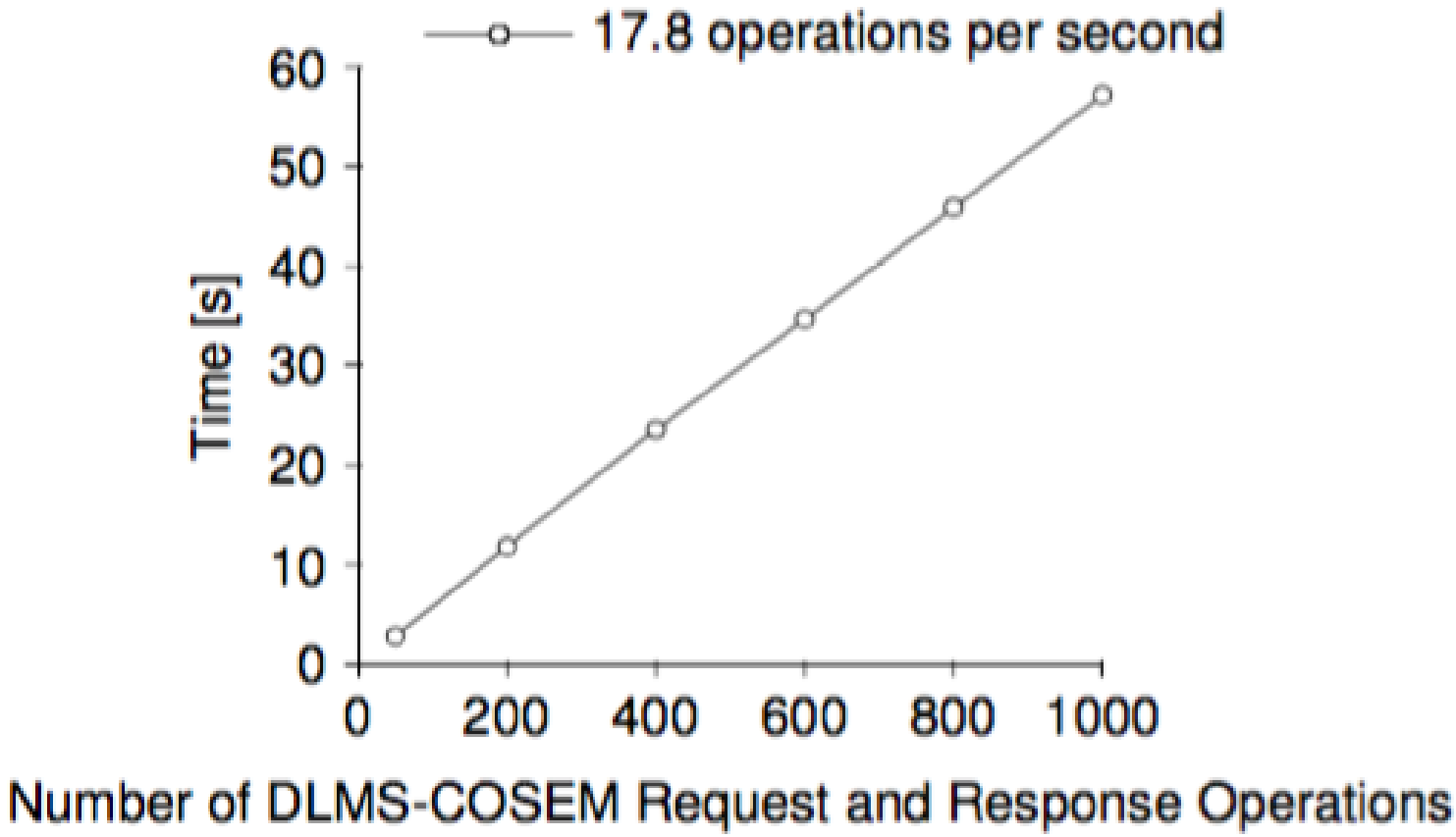

## Skylake SGX machine

- Dell Latitude E5570
- June 2016 SGX SDK
- Basic Network
- Simulated SMDs
- DLMS-COSEM

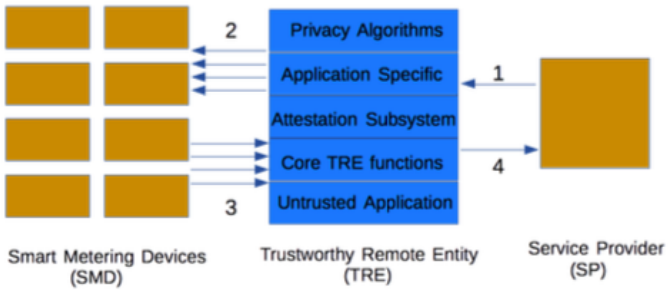
# Results: Comparison of TPM-based and SGX-based

| | TPM-TRE | SGX-TRE |
|---|---|---|
| Crypto Libraries | 14,408 | 2,529 |
| Communication | 5,969 | 858 |
| Memory Management | 1,035 | 774 |
| C/C++ Library | 854 | 7,528 |
| Core TRE | 720 | 229 |
| Application Specific | 507 | 507 |
| Attestation | 221 | 364 |
| Drivers | 1,005 | - |
| SGX Trusted | - | 2,968 |
| Total | 24,719 | 15,757 |

# Results: Performance of SGX-based TRE



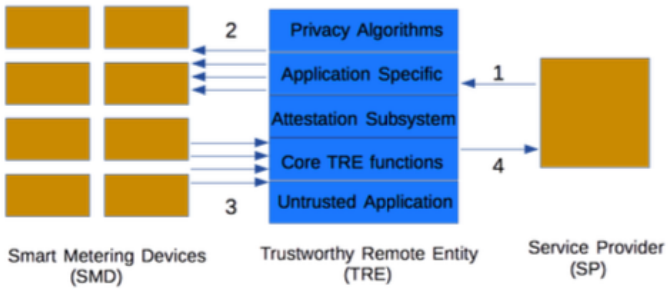
# Security Evaluation




## SGX-based TRE

- No Outside Calls
- No Secret dependent access patterns
- SGX features.

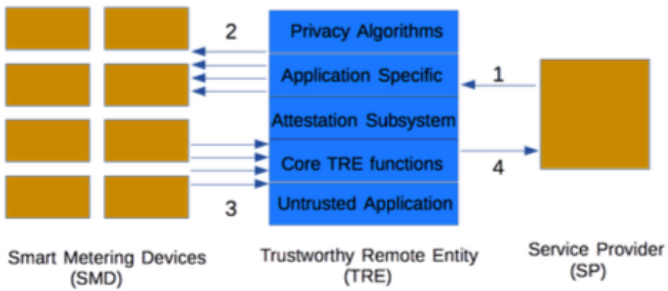
# Conclusion




## SGX-based TRE

- Template for Many Party apps
- Comparison of approaches
- Smaller TCB
- Stronger Adversary

# Questions




Any comments?